নাম: _____ তারিখ: _____ নম্বর: _____

জিরো ট্রাস্ট আর্কিটেকচার ও নিরাপত্তা

ধারাবাহিক যাচাইকরণ, নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন, আইডেন্টিটি ও অ্যাক্সেস ম্যানেজমেন্ট, ন্যূনতম সুবিধা এবং অবস্থান-যাচাই।

জিরো ট্রাস্ট নিরাপত্তা শিক্ষার সারসংক্ষেপ

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে Zero Trust আর্কিটেকচার ও নিরাপত্তা বিষয়ে গাইড করবে। আপনি ক্রমাগত যাচাই, নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন, আইডেন্টিটি অ্যাক্সেস ম্যানেজমেন্ট (IAM), ন্যূনতম বিশেষাধিকার ও সেশন অডিটিং সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/zero-trust-cyber-security/

আপনার জিরো ট্রাস্ট কৌশল শেখার রোডম্যাপ

- ক্রমাগত যাচাইয়ের মূল নীতি বুঝুন।
- নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন এবং ন্যূনতম সুবিধার অ্যাক্সেস বাস্তবায়ন করুন।
- ডিভাইস অবস্থান-যাচাই ও সক্রিয় সেশন নিরীক্ষা কনফিগার করুন।

জিরো ট্রাস্ট নিরাপত্তা নির্দেশিকার নির্দেশাবলি

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। Zero Trust আর্কিটেকচার বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

জিরো ট্রাস্ট আর্কিটেকচার ও নিরাপত্তা (ভূমিকা)

Zero Trust নিরাপত্তা পুরনো নেটওয়ার্ক পরিসীমা মডেলের জায়গায় কঠোর 'কাউকে বিশ্বাস নয়, সবসময় যাচাই' নীতি আনে। মাইক্রো-সেগমেন্টেশন, Identity and Access Management (IAM), ন্যূনতম সুবিধার অধিকার এবং পোশ্চার চেক বাস্তবায়ন পার্শ্বীয় হুমকি চলাচল ঠেকায়।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. জিরো ট্রাস্ট নিরাপত্তার মূল নীতি কী?**

- A. কখনো বিশ্বাস নয়, উৎস যা-ই হোক প্রতিটি অ্যাক্সেস অনুরোধ সবসময় যাচাই করা
- B. কর্পোরেট ফায়ারওয়ালের ভেতরের সব ট্র্যাফিককে নিরাপদ ধরে নেওয়া
- C. গতি বাড়াতে এনক্রিপশন ছাড়া ডাটাবেস ফাইল সংরক্ষণ করা
- D. শুধু SPF রেকর্ড ব্যবহার করে ইমেইল প্রমাণীকরণ কার্যকর করা

2 **2. নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন কী?**

- A. পার্শ্বীয় চলাচল আটকাতে নেটওয়ার্ককে ছোট, বিচ্ছিন্ন অঞ্চলে ভাগ করা
- B. ডেটা ট্রানজিটের সময় নেটওয়ার্ক কার্ড এনক্রিপ্ট করা
- C. সব স্থানীয় সার্ভারকে একটিমাত্র পাবলিক IP ঠিকানার সঙ্গে যুক্ত করা
- D. ব্রাউজার সেশনে ব্যবহারকারীর কিস্ট্রোক পর্যবেক্ষণ করা

3 **3. ন্যূনতম সুযোগ-সুবিধার নীতি (principle of least privilege) কী?**

- A. ব্যবহারকারীর কাজের জন্য যতটুকু প্রয়োজন, শুধু ততটুকুতে প্রবেশের অনুমতি সীমিত করা
- B. ডিফল্টভাবে প্রতিটি ব্যবহারকারীকে সব সিস্টেম সুবিধা দেওয়া
- C. কর্পোরেট ডেটাবেস সার্ভারে বেনামি লগইনের অনুমতি দেওয়া
- D. পাসওয়ার্ড ছাড়া পাবলিক Wi-Fi রাউটার কনফিগার করা

4 **4. আইডেন্টিটি অ্যান্ড অ্যাক্সেস ম্যানেজমেন্ট (IAM) কী?**

- A. ডিজিটাল পরিচয় ব্যবস্থাপনা ও সিস্টেম সুবিধা নিয়ন্ত্রণ করা কাঠামো
- B. স্থানীয় ফাইল ডিরেক্টরি স্ক্যান করা অ্যান্টিভাইরাস ইউটিলিটি
- C. এয়ার-গ্যাপড মিডিয়া ব্যবহার করা ব্যাকআপ স্টোরেজ সিস্টেম
- D. স্পুফ করা ডোমেইন প্রত্যাখ্যানকারী একটি ইমেইল গেটওয়ে প্রোটোকল

5 **5. কন্টিনিউয়াস অথেনটিকেশন বলতে কী বোঝায়?**

- A. সক্রিয় সেশনের সময় বারবার ব্যবহারকারীর পরিচয় ও ডিভাইসের অবস্থা যাচাই করা
- B. প্রতি 10 মিনিটে মাস্টার পাসওয়ার্ড পরিবর্তন করা
- C. একাধিক অ্যালগরিদম দিয়ে ডাটাবেস রেকর্ড হ্যাশ করা
- D. TLS কী ব্যবহার করে নেটওয়ার্ক পরিবহন প্যাকেট এনক্রিপ্ট করা

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. Zero Trust ধরে নেয় যে কর্পোরেট ফায়ারওয়ালের ভেতরের সব ট্রাফিক নিরাপদ।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. মাইক্রো-সেগমেন্টেশন আক্রমণকারীদের অভ্যন্তরীণ সার্ভারজুড়ে পার্শ্বীয় গতিবিধির সক্ষমতা সীমিত করে।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. ন্যূনতম বিশেষাধিকার ডিফল্টভাবে সব ডাটাবেস ফাইলে অ্যাক্সেস দেয়।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. ধারাবাহিক যাচাইকরণ একটি লগইন সেশনজুড়ে ডিভাইসের স্বাস্থ্য ও ক্রেডেনশিয়াল যাচাই করে।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. Zero Trust বাস্তবায়ন কর্পোরেট লগইন ফাঁসের প্রভাব কমায়।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. প্রতিটি প্রবেশ-বিন্দুতে পরিচয়-তথ্য চাওয়া হলো ধারাবাহিক _____ ।
2. কর্পোরেট নেটওয়ার্ককে ক্ষুদ্র ক্ষুদ্র অঞ্চলে ভাগ করা হলো মাইক্রো- _____ ।
3. ডিজিটাল পরিচয় ও অ্যাক্সেস নিয়ন্ত্রণ কনফিগার করতে একটি _____ ব্যবস্থা ব্যবহৃত হয়।
4. ব্যবহারকারীর অনুমতি সীমিত করতে ব্যবহৃত হয় ন্যূনতম _____ -এর নীতি।
5. সংযুক্ত ডিভাইসের স্বাস্থ্য মূল্যায়নে ডিভাইসের _____ স্ক্যান করা হয়।
6. সক্রিয় সেশন লগ করা ও পর্যালোচনা করা হলো নিরাপত্তা _____ ।

পরিভাষা শব্দভাণ্ডার

অডিটিং অধিকার অবস্থা আইএএম ফায়ারওয়াল যাচাইকরণ রাউটার সেগমেন্টেশন

এখানে আপনার উত্তর লিখুন:

1.
2.
3.
4.
5.
6.

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

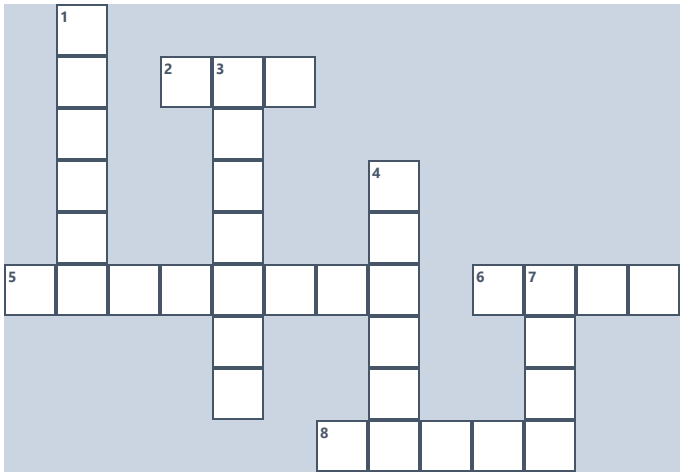
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

☐	**1. যাচাইকরণ**	**A**	ব্যবহারকারীর ক্রেডেনশিয়াল অ্যাক্সেস পরিচালনা।
☐	**2. সেগমেন্টেশন**	**B**	ন্যূনতম অ্যাক্সেস অধিকারের নীতি।
☐	**3. IAM**	**C**	নেটওয়ার্ক প্যাকেট ট্রাফিক রাউটিং।
☐	**4. প্রিভিলেজ**	**D**	বাইরের নেটওয়ার্ক প্রাচীর সুরক্ষা।
☐	**5. পোস্চার**	**E**	লগ করা অ্যাক্সেস সেশন পর্যালোচনা।
☐	**6. নিরীক্ষা চালানো**	**F**	অভ্যন্তরীণ নেটওয়ার্ক জোন বিভক্ত করা।
☐	**7. ফায়ারওয়াল**	**G**	সবসময় ব্যবহারকারীর ক্রেডেনশিয়াল যাচাই করা।
☐	**8. রাউটার**	**H**	ডিভাইসের স্বাস্থ্য অবস্থা মূল্যায়ন।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

2. লগ করা অ্যাক্সেস সেশন পর্যালোচনা (3)

5. সবচেয়ে কম অ্যাক্সেস-অধিকারের নীতি (8)

6. ডেটা ও ব্যবহারকারীকে ঝুঁকি থেকে সুরক্ষার ব্যবস্থা (4)

8. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5)

উপর-নিচ

1. অভ্যন্তরীণ নেটওয়ার্ক অঞ্চল ভাগ করা (6)

3. ডিভাইসের স্বাস্থ্য-অবস্থা মূল্যায়ন (7)

4. বাইরের নেটওয়ার্ক-প্রতিরোধ সুরক্ষা (6)

7. নেটওয়ার্ক প্যাকেট ট্র্যাফিকের পথ নির্ধারণ (4)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

2 পাশাপাশি: লগ করা অ্যাক্সেস সেশন পর্যালোচনা (3 অক্ষর):

5 পাশাপাশি: সবচেয়ে কম অ্যাক্সেস-অধিকারের নীতি (8 অক্ষর):

6 পাশাপাশি: ডেটা ও ব্যবহারকারীকে ঝুঁকি থেকে সুরক্ষার ব্যবস্থা (4 অক্ষর):

8 পাশাপাশি: ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর):

উপর-নিচ

1 উপর-নিচ: অভ্যন্তরীণ নেটওয়ার্ক অঞ্চল ভাগ করা (6 অক্ষর):

3 উপর-নিচ: ডিভাইসের স্বাস্থ্য-অবস্থা মূল্যায়ন (7 অক্ষর):

4 উপর-নিচ: বাইরের নেটওয়ার্ক-প্রতিরোধ সুরক্ষা (6 অক্ষর):

7 উপর-নিচ: নেটওয়ার্ক প্যাকেট ট্র্যাফিকের পথ নির্ধারণ (4 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

স ন ঝ কা জ রা ফ নি ঘ উ সে জি আ ড প
পা শ ধ দ জি কি না রা ম্যা লি ই রে ফ চ ব
দি ন্টে শ জা রা দে ট প মে ল র ক সি দ ঠ
হ মে সা শ মে দে রা ত্তা কি ঋ ও তে না নে ছ
য গ প উ অ ন্যূ উ ঋ মা বা অ য়্যা য রা ফ
বা সে ম দে তি ন ভ ডি ঘ রে ষ ডি র উ ফ
ল ঘ দ হ স ত ভ রি ভা মি ঢ ষ টিং টা ষ
য়া রি সি না তি ম তা ড ঊ ই নি রা কি র থ
ও সে ঊ লি গ অ নি জা পি ঋ স জি লি ট ভ
র ণ জে গ স ধি ঘ রে দি মি ঋ অ পা উ অ
য়া জে কা গ ম কা আ ঘ কি ঘ ঝ ণ ব ধ গ
ফা সি রি শ ছ র দ সে জি নি ঝ রে পে স্থা জ
আ আ রে মা স মে তি দে রি ফ সি তি সে খ স
বে উ ট সে দি দা প আ সি জে বি বি য ড দ
ষ সা ফ ল ল তা কে ণ রা রি ণ জে ই কে পে

পরিভাষা শব্দতালিকা

সেগমেন্টেশন ন্যূনতমঅধিকার ডিভাইসঅবস্থা অডিটিং ফায়ারওয়াল রাউটার ম্যালওয়্যার নিরাপত্তা

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. সেগমেন্টেশন

B. ন্যূনতমঅধিকার

C. ডিভাইসঅবস্থা

D. অডিটিং

E. ফায়ারওয়াল

F. রাউটার

G. ম্যালওয়্যার

H. নিরাপত্তা

সংজ্ঞা ও মিলের ঘর

1. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার।
2. নেটওয়ার্ক প্যাকেট ট্র্যাফিকের পথ নির্ধারণ।
3. লগ করা অ্যাক্সেস সেশন পর্যালোচনা।
4. সবচেয়ে কম অ্যাক্সেস-অধিকারের নীতি।
5. ডেটা ও ব্যবহারকারীকে ঝুঁকি থেকে সুরক্ষার ব্যবস্থা।
6. বাইরের নেটওয়ার্ক-প্রতিরোধ সুরক্ষা।
7. ডিভাইসের স্বাস্থ্য-অবস্থা মূল্যায়ন।
8. অভ্যন্তরীণ নেটওয়ার্ক অঞ্চল ভাগ করা।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. মে সে ন্টে শ ন গ
2. ডি ই স্থা ব অ স ভা
3. ফা র ও ল য়া য়া
4. ও র য়্যা ম্যা ল
5. অ ধি ন র ম ন্যূ কা ত
6. ডি টিং অ
7. টা রা র উ
8. নি ত্তা প রা

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
2	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
3	একটি ডিভাইসে যা যা যাচাই করা হয়			
4	যেসব জিনিস লগ করা হয়			
5	সাইবার নিরাপত্তার সঙ্গে সম্পর্কিত শব্দ			
6	Zero Trust যা যা যাচাই করে			
7	দৈনন্দিন জীবনে যেসব জায়গায় আপনি পরিচয়পত্র দেখান			
8	আপনি আসলেই আপনি তা প্রমাণ করার উপায়			
9	ডেটা ফাঁসের পর যা করবেন			
10	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
11	সফটওয়্যার আপডেট করার কারণ			
12	একটি কোম্পানির অ্যাক্সেস স্তর			
13	আপনার জানা নিরাপত্তা টুল			
14	একটি নেটওয়ার্ককে যেসব জোনে ভাগ করা যায়			
15	আস্থা নিয়ে প্রবাদ বা উক্তি			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: জিরো ট্রাস্ট নেটওয়ার্ক আর্কিটেকচারে রূপান্তর



পরিস্থিতি: একটি বড় এন্টারপ্রাইজ বর্তমানে একটি ফ্ল্যাট অভ্যন্তরীণ নেটওয়ার্ক ব্যবহার করে, যেখানে লোকাল নেটওয়ার্কের যেকোনো ডিভাইস সব কর্পোরেট সার্ভার ও ডেটাবেসে ঢুকতে পারে।

আলোচনার প্রশ্ন: পার্শ্বীয় গতিবিধি সীমিত করতে একটি নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন কৌশল ডিজাইন করুন।

কেস স্টাডি 2: ন্যূনতম সুবিধা প্রবেশ নিয়ন্ত্রণ স্থাপন



পরিস্থিতি: অডিট লগে দেখা যায় যে অস্থায়ী ডেটাবেস ব্যবহারকারী ও নিম্নস্তরের কর্মীদের গুরুত্বপূর্ণ হিসাবরক্ষণ ডেটাবেসে গ্লোবাল রিড ও রাইট অনুমতি আছে।

আলোচনার প্রশ্ন: ন্যূনতম সুবিধার নীতি কার্যকর করতে ডেটাবেস IAM সুবিধাগুলো অডিট করুন এবং সীমিত করুন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12
খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24
ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36
য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48
ূ=49 ৃ=50 ে=51 ৈ=52 ো=53 ৌ=54 ং=55 ঃ=56 ঁ=57 ্=58 ়=59

19	46	38	53		22	58	38	45	42	58	22

42	58	28	45	32	27	58	37	51		42	34	42	36	37	59

37	45	17	45	3		12	38	48	31

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: Zero Trust কী?

Zero Trust একটি নিরাপত্তা কাঠামো, যা ধরে নেয় যে হুমকি নেটওয়ার্ক সীমানার বাইরে ও ভেতরে দুই জায়গাতেই থাকে, এবং প্রতিটি অনুরোধের জন্য যাচাই চায়। [1]

Q2: Zero Trust-এর মূল নিয়ম কী?

কখনও আস্থা নয়, সবসময় যাচাই।

Q3: মাইক্রো-সেগমেন্টেশন কী?

ট্রাফিক নিয়ন্ত্রণ ও ব্রিচ সীমাবদ্ধ রাখতে নেটওয়ার্ককে ছোট, নিরাপদ যৌক্তিক অংশে ভাগ করা।

Q4: লিস্ট প্রিভিলেজ কী?

ব্যবহারকারীদের কেবল তাদের নির্দিষ্ট কাজ সম্পাদনের জন্য প্রয়োজনীয় ন্যূনতম অ্যাক্সেস অধিকার দেওয়া। [2]

Q5: IAM-এর পূর্ণরূপ কী?

আইডেন্টিটি অ্যান্ড অ্যাক্সেস ম্যানেজমেন্ট।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: ডিভাইস পোসচার চেক কীভাবে সাহায্য করে?

অ্যাক্সেস দেওয়ার আগে এটি যাচাই করে যে ডিভাইসটি প্যাচ করা, সক্রিয় অ্যান্টিভাইরাস চালাচ্ছে এবং নিরাপদ।

Q7: ল্যাটারাল মুভমেন্ট কী?

আক্রমণকারীরা প্রাথমিকভাবে দখল করা নোড থেকে নেটওয়ার্কের মধ্য দিয়ে বেশি মূল্যবান সিস্টেমে যে প্রক্রিয়ায় এগিয়ে যায়।

Q8: জিরো ট্রাস্ট কি ফায়ারওয়াল প্রতিস্থাপন করে?

না, এটি পরিচয়-কেন্দ্রিক যাচাই ও অভ্যন্তরীণ সেগমেন্টেশন ফায়ারওয়াল যোগ করে সেগুলোকে আরও বাড়ায়।

Q9: কন্টিনিউয়াস অথেনটিকেশন কী?

শুধু প্রথম সাইন-ইনের সময় নয়, সক্রিয় লগইন সেশনজুড়ে ব্যবহারকারীর পরিচয়ের ধারাবাহিক যাচাই।

Q10: ফ্ল্যাট নেটওয়ার্ক বিপজ্জনক কেন?

ফ্ল্যাট নেটওয়ার্কে একটি আপসকৃত নোড আক্রমণকারীদের নেটওয়ার্কের যেকোনো ডেটাবেসে সহজে প্রবেশের সুযোগ দেয়।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: Zero Trust কীভাবে পরিসীমা-ভিত্তিক মডেলের সমস্যা মোকাবিলা করে?

এটি পুরোনো 'castle-and-moat' মডেলের স্থলাভিষিক্ত হয়, প্রতিরক্ষাকে সীমানা নেটওয়ার্ক থেকে নির্দিষ্ট ব্যবহারকারীর পরিচয় ও রিসোর্সে সরিয়ে আনে।

Q2: পলিসি ডিসিশন পয়েন্ট (PDP) কী?

সিস্টেমের যে অংশ নিরাপত্তা নিয়মের বিরুদ্ধে অনুমোদনের অনুরোধ যাচাই করে সিদ্ধান্ত নেয় অ্যাক্সেস দেওয়া হবে কি না।

Q3: পলিসি এনফোর্সমেন্ট পয়েন্ট (PEP) কী?

সিস্টেম নোড (যেমন গেটওয়ে বা প্রক্সি), যা PDP-র সিদ্ধান্ত অনুযায়ী বাস্তবে সংযোগের অনুরোধ অনুমোদন বা ব্লক করে।

Q4: রোল-বেইজড অ্যাক্সেস কন্ট্রোল (RBAC) কীভাবে জিরো ট্রাস্টকে সমর্থন করে?

RBAC অনুমতিগুলোকে নির্দিষ্ট ভূমিকায় গোষ্ঠীবদ্ধ করে, যা ব্যবহারকারীদের অতিরিক্ত প্রশাসনিক ক্ষমতা উত্তরাধিকারসূত্রে পাওয়া ঠেকাতে সাহায্য করে।

Q5: কনটেক্সচুয়াল অ্যাক্সেস কন্ট্রোল কী?

ঝুঁকি যাচাইয়ে ভৌগোলিক অবস্থান, ডিভাইস পোশ্চার ও লগইনের সময়ের মতো গৌণ সূত্র দিয়ে লগইন অনুরোধ মূল্যায়ন।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: মাইক্রো-সেগমেন্টেশন সাধারণ VLAN থেকে কীভাবে আলাদা?

VLAN লেয়ার 2-এ নেটওয়ার্ককে বিস্তৃত যৌক্তিক অংশে ভাগ করে, আর মাইক্রো-সেগমেন্টেশন সফটওয়্যার পলিসি ব্যবহার করে আলাদা আলাদা ওয়ার্কলোডকে বিচ্ছিন্ন করে।

Q7: জাস্ট-ইন-টাইম (JIT) অ্যাক্সেস কী?

সাময়িকভাবে উচ্চ প্রশাসনিক অনুমতি দেওয়া এবং কাজ শেষ হলে স্বয়ংক্রিয়ভাবে তা প্রত্যাহার করা।

Q8: জিরো ট্রাস্ট ফ্রেমওয়ার্কে আপনি কীভাবে API সুরক্ষিত করবেন?

ক্রিপ্টোগ্রাফিক স্বাক্ষরিত OAuth টোকেন আবশ্যক করে এবং প্রতিটি API গেটওয়েতে অনুরোধের স্বাক্ষর অডিট করে।

Q9: জিরো-ট্রাস্ট নেটওয়ার্ক অ্যাক্সেস (ZTNA) ক্লায়েন্ট কী?

র নেটওয়ার্ক সাবনেটের বদলে নির্দিষ্ট অ্যাপ্লিকেশনে নিরাপদ, এনক্রিপ্টেড বহির্গামী সংযোগ স্থাপন করা একটি সফটওয়্যার এজেন্ট।

Q10: লগ অডিটিং কীভাবে Zero Trust-কে সাহায্য করে?

ধারাবাহিক লগিং স্বয়ংক্রিয় নিরাপত্তা বিশ্লেষণ টুলকে অস্বাভাবিকতা শনাক্ত করতে এবং ক্ষতিকর লগইন সঙ্গে সঙ্গে স্থগিত করতে দেয়।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

Zero Trust আর্কিটেকচার পুরনো ক্যাসল-অ্যান্ড-মোট মডেলের জায়গায় পরিচয়-কেন্দ্রিক যাচাই নিয়ম আনে।

2. নিরাপত্তা ইনসাইট

নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন ওয়ার্কলোডকে ছোট সুরক্ষিত জোনে আলাদা করে ম্যালওয়্যার যতদূর পৌঁছাতে পারে সেই এলাকা ছোট করে।

3. নিরাপত্তা ইনসাইট

Zero Trust নেটওয়ার্ক সেগমেন্টের বদলে সম্পদ, পরিষেবা ও অ্যাকাউন্টের মতো রিসোর্স সুরক্ষায় মনোযোগ দেয়। [1]

4. নিরাপত্তা ইনসাইট

ন্যূনতম বিশেষাধিকার অ্যাক্সেস নীতি মূল ডাটাবেস থেকে অভ্যন্তরীণ হুমকির তথ্য বেরিয়ে যাওয়ার ঝুঁকি কমায়।

5. নিরাপত্তা ইনসাইট

ডিভাইস পোশ্চার যাচাই রিয়েল টাইমে অপারেটিং সিস্টেমের প্যাচ স্তর ও সক্রিয় অ্যান্টিভাইরাসের অবস্থা পরীক্ষা করে।

6. নিরাপত্তা ইনসাইট

Zero Trust Network Access (ZTNA) ব্রোকার ব্যবহারকারীর অ্যাক্সেসের পরিধি সীমিত করতে কর্পোরেট VPN-এর বিকল্প বা পরিপূরক হতে পারে।

7. সিকিউরিটি ইনসাইট

জাস্ট-ইন-টাইম (JIT) প্রশাসনিক সুবিধা অর্পণ ডোমেইন কন্ট্রোলারে লগইন তথ্য চুরির ঝুঁকি কমায়।

8. সিকিউরিটি ইনসাইট

ধারাবাহিক যাচাইকরণ লগ রাখে ও সেশনের আচরণ নিরীক্ষা করে, এবং অস্বাভাবিক স্ক্রিপ্ট কার্যকরের ধরন দেখানো ব্যবহারকারীদের স্থগিত করে।

9. সিকিউরিটি ইনসাইট

প্রশাসনিক ক্রেডেনশিয়াল ফাঁস হয়ে গেলে প্রচলিত পরিসীমা প্রতিরক্ষা পার্শ্বীয় আক্রমণ ঠেকাতে ব্যর্থ হয়।

10. নিরাপত্তা ইনসাইট

NIST Special Publication 800-207 (2020) ডিপ্লয়মেন্ট মডেলসহ জিরো ট্রাস্ট আর্কিটেকচারের একটি বিমূর্ত সংজ্ঞা দেয়। [1]

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 সঠিক উত্তর: A

শিক্ষণ নোট

জিরো ট্রাস্ট নিরাপত্তার মূল নীতি কী? → কখনো বিশ্বাস নয়, উৎস যা-ই হোক প্রতিটি অ্যাক্সেস অনুরোধ সবসময় যাচাই করা

2 প্রশ্ন 2 সঠিক উত্তর: A

শিক্ষণ নোট

নেটওয়ার্ক মাইক্রো-সেগমেন্টেশন কী? → পার্শ্বীয় চলাচল আটকাতে নেটওয়ার্ককে ছোট, বিচ্ছিন্ন অঞ্চলে ভাগ করা

3 প্রশ্ন 3 সঠিক উত্তর: A

শিক্ষণ নোট

ন্যূনতম সুযোগ-সুবিধার নীতি (principle of least privilege) কী? → ব্যবহারকারীর কাজের জন্য যতটুকু প্রয়োজন, শুধু ততটুকুতে প্রবেশের অনুমতি সীমিত করা

4 প্রশ্ন 4 সঠিক উত্তর: A

শিক্ষণ নোট

আইডেন্টিটি অ্যান্ড অ্যাক্সেস ম্যানেজমেন্ট (IAM) কী? → ডিজিটাল পরিচয় ব্যবস্থাপনা ও সিস্টেম সুবিধা নিয়ন্ত্রণ করা কাঠামো

5 প্রশ্ন 5 সঠিক উত্তর: A

শিক্ষণ নোট

কন্টিনিউয়াস অথেনটিকেশন বলতে কী বোঝায়? → সক্রিয় সেশনের সময় বারবার ব্যবহারকারীর পরিচয় ও ডিভাইসের অবস্থা যাচাই করা

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: Zero Trust নেটওয়ার্কের ভেতরে বা বাইরে অবস্থানের ভিত্তিতে কোনো অন্তর্নিহিত আস্থা দেয় না।

7 প্রশ্ন 7 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: ছোট বিচ্ছিন্ন জোন একজন অনুপ্রবেশকারী সার্ভারগুলোর মধ্যে কতদূর যেতে পারে তা সীমিত করে।

8 প্রশ্ন 8 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: ন্যূনতম সুবিধার নীতি প্রতিটি ভূমিকাকে কেবল প্রয়োজনীয় ন্যূনতম অ্যাক্সেস দেয়।

9 প্রশ্ন 9 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

ধারাবাহিক যাচাইকরণ একটি লগইন সেশনজুড়ে ডিভাইসের স্বাস্থ্য ও ক্রেডেনশিয়াল যাচাই করে।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

Zero Trust বাস্তবায়ন কর্পোরেট লগইন ফাঁসের প্রভাব কমায়।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

G 1. যাচাইকরণ	F 2. সেগমেন্টেশন	A 3. IAM	B 4. প্রিভিলেজ
H 5. পোস্চার	E 6. নিরীক্ষা চালানো	D 7. ফায়ারওয়াল	C 8. রাউটার

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 যাচাইকরণ	2 সেগমেন্টেশন	3 আইএএম	4 অধিকার
5 অবস্থা	6 অডিটিং		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 G – ম্যালওয়্যার	2 F – রাউটার	3 D – অডিটিং	4 B – ন্যূনতমঅধিকার
5 H – নিরাপত্তা	6 E – ফায়ারওয়াল	7 C – ডিভাইসঅবস্থা	8 A – সেগমেন্টেশন

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা যাচাইকরণ, সেগমেন্টেশন ও IAM নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

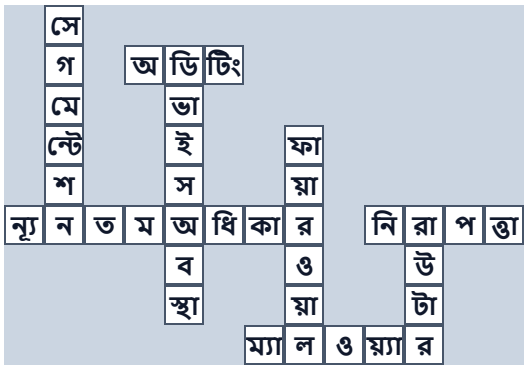
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

স	ন	ঝ	কা	জ	রা	ফ	নি	ঘ	উ	সে	জি	আ	ড	প
পা	শ	ধ	দ	জি	কি	না	রা	ম্যা	লি	ই	রে	ফ	চ	ব
দি	ন্টে	শ	জা	রা	দে	ট	প	মে	ল	র	ক	সি	দ	ঠ
হ	মে	সা	শ	মে	দে	রা	ত্তা	কি	ঋ	ও	তে	না	নে	ছ
য	গ	প	উ	অ	ন্যূ	উ	ঋ	মা	বা	অ	য়্যা	য	রা	ফ
বা	সে	ম	দে	তি	ন	ভ	ডি	ঘ	রে	ষ	ডি	র	উ	ফ
ল	ঘ	দ	হ	স	ত	ভ	রি	ভা	মি	ঢ	ষ	টিং	টা	ষ
য়া	রি	সি	না	তি	ম	তা	ড	ঊ	ই	নি	রা	কি	র	থ
ও	সে	ঊ	লি	গ	অ	নি	জা	পি	ঋ	স	জি	লি	ট	ভ
র	ণ	জে	গ	স	ধি	ঘ	রে	দি	মি	ঋ	অ	পা	উ	অ
য়া	জে	কা	গ	ম	কা	আ	ঘ	কি	ঘ	ঝ	ণ	ব	ধ	গ
ফা	সি	রি	শ	ছ	র	দ	সে	জি	নি	ঝ	রে	পে	স্থা	জ
আ	আ	রে	মা	স	মে	তি	দে	রি	ফ	সি	তি	সে	খ	স
বে	উ	ট	সে	দি	দা	প	আ	সি	জে	বি	বি	য	ড	দ
ষ	সা	ফ	ল	ল	তা	কে	ণ	রা	রি	ণ	জে	ই	কে	পে

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

2 পাশাপাশি: অডিটিং লগ করা অ্যাক্সেস সেশন পর্যালোচনা (3 অক্ষর)

5 পাশাপাশি: ন্যূনতমঅধিকার সবচেয়ে কম অ্যাক্সেস-অধিকারের নীতি (8 অক্ষর)

6 পাশাপাশি: নিরাপত্তা ডেটা ও ব্যবহারকারীকে ঝুঁকি থেকে সুরক্ষার ব্যবস্থা (4 অক্ষর)

8 পাশাপাশি: ম্যালওয়্যার ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর)

উপর-নিচ

1 উপর-নিচ: সেগমেন্টেশন অভ্যন্তরীণ নেটওয়ার্ক অঞ্চল ভাগ করা (6 অক্ষর)

3 উপর-নিচ: ডিভাইসঅবস্থা ডিভাইসের স্বাস্থ্য-অবস্থা মূল্যায়ন (7 অক্ষর)

4 উপর-নিচ: ফায়ারওয়াল বাইরের নেটওয়ার্ক-প্রতিরোধ সুরক্ষা (6 অক্ষর)

7 উপর-নিচ: রাউটার নেটওয়ার্ক প্যাকেট ট্র্যাফিকের পথ নির্ধারণ (4 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1.	মেসেন্টেশনগ	সেগমেন্টেশন	5.	অধিনরমন্যূকাত	ন্যূনতমঅধিকার
2.	ডিইস্থাবঅসভা	ডিভাইসঅবস্থা	6.	ডিটিংঅ	অডিটিং
3.	ফারওলয়ায়া	ফায়ারওয়াল	7.	টারারউ	রাউটার
4.	ওরয়্যাম্যাল	ম্যালওয়্যার	8.	নিত্তাপরা	নিরাপত্তা

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"জিরো ট্রাস্ট স্থাপত্যে সবসময় যাচাই করুন"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: জিরো ট্রাস্ট নেটওয়ার্ক আর্কিটেকচারে রূপান্তর

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি বড় এন্টারপ্রাইজ বর্তমানে একটি ফ্ল্যাট অভ্যন্তরীণ নেটওয়ার্ক ব্যবহার করে, যেখানে লোকাল নেটওয়ার্কের যেকোনো ডিভাইস সব কর্পোরেট সার্ভার ও ডেটাবেসে প্রবেশ করতে পারে।
- প্রস্তাবিত কৌশল ও সমাধান: ফ্ল্যাট নেটওয়ার্ককে বিচ্ছিন্ন বিভাগীয় জোনে ভাগ করুন। জোনগুলোর মধ্যকার ট্রাফিক নিয়ন্ত্রণে অভ্যন্তরীণ ফায়ারওয়াল বসান এবং সব প্রবেশাধিকারের জন্য সংযোগ টোকেন যাচাই বাধ্যতামূলক করুন।

B কেস স্টাডি 2: ন্যূনতম সুবিধা প্রবেশ নিয়ন্ত্রণ স্থাপন

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: অডিট লগ থেকে দেখা যায়, অস্থায়ী ডেটাবেস ব্যবহারকারী ও নিম্নস্তরের কর্মীদের গুরুত্বপূর্ণ হিসাব-সংক্রান্ত ডেটাবেসে বৈশ্বিক পড়া ও লেখার অনুমতি রয়েছে।
- প্রস্তাবিত কৌশল ও সমাধান: সব বৈশ্বিক প্রশাসনিক সুবিধা বাতিল করুন। কাজের ভূমিকার সঙ্গে সঠিকভাবে মিলিয়ে Role-Based Access Control (RBAC) চালু করুন এবং সাপ্তাহিক স্বয়ংক্রিয় অনুমতি পর্যালোচনা প্রতিষ্ঠা করুন।